"Truth in Caller ID Act of 2006"
Re: H.R. 5126
May 16th, 2006

The "Truth in Caller ID Act of 2006" is being introduced with the goal of preventing criminal activities and/or the obstruction of justice with respect to the manipulation of caller identification information.

As one of the founders of Secure Science Corporation, an Internet security and research company, I have personally witnessed the extent to which the abuse and misuse of caller ID can have. In August of 2004, our investigation team discovered that two of the Nation's largest telecommunications providers (T-mobile, Verizon) were vulnerable to a technique known as "Caller-ID Spoofing". This technique is entirely reliant upon the manipulation of Caller ID to be successful and enables the attacker access to individual customer's voicemail without using a PIN code, violating both customer privacy and authentication protocols to cellular and land-line voice mail networks. Similar intrusions, also known as "exploits", include unauthorized termination of customer accounts, anonymous automatic phone SPAM, and the potential to gain full administrative control over a major telecommunications network that serves both business and residential phone lines. This last possibility is one of the greatest concerns in conjunction with the inappropriate and unlawful uses of caller ID and could even be viewed as a threat to national security in much the same way as the destabilization of a utilities plant or traffic control station would be.

Other exploits employing Caller ID Spoofing have been used by criminals who con unsuspecting victims out of money and in many cases their identity (also called "Phishers" and their methods "Phishing"). This activity involves the utilization of information gained illegally by breaking into a potential victim's voice mail account. This in turn allows the phishers to further victimize customers by using, for example, billing information to steal identities and garner even more personal information from other sources. Conversely, Phishers will use Caller ID Spoofing in order to pose as a victim's bank and phish the account via phone. This same method is also used to lure wire transfer delivery services (such as Western Union) into authorizing fraudulent transfers over the phone. Additionally, Phishers will verify their access to the stolen accounts by using the victim's contact numbers in an attempt to validate account availability and amounts.

Because of the level and quantity of illegal activities participated in by Phishers, anonymity is one of their primary objectives. Caller ID Spoofing enables them to not only communicate covertly with one another, but also provides them with an advantage against law enforcement agencies. As a direct result, the Phishers continue their operations all the while evading subpoena attempts.

The aforementioned instances are just some of the many ways in which the fraudulent

uses of Caller ID are being employed today. Our company's research alone demonstrates that more than 75% of the transactions and/or spoofed calls made on providers' networks were with mal-intent.

Despite the dark side of Caller ID Spoofing, there are very tangible benefits associated with this technique when used in a responsible manner. Secure Science Corporation is often called upon to assist companies who provide automated Caller ID Spoofing services to detect and prevent fraudulent activity on their network. In order to do this successfully, it is not unusual for us to aid law enforcement by using Caller-ID Spoofing techniques to track down these perpetrators. By accessing the very information they attempt to conceal, Phishers and other such criminals are not successful in their evasive actions, thus increasing the amount of successful investigations with law enforcement involvement brought forth against them.

One of the most common reasons for the manipulation of Caller ID information is executed by the vast majority of Voice-Over-IP companies, as well as those businesses which use Private Branch Exchanges, better known as PBX's. In this case they appropriately utilize the technique so as to provide their telephone communications users with a viable and fiscally prudent alternative to traditional long distance services. One such legitimate use of Caller ID Spoofing is the transmission of the caller’s home telephone number on a Voice-over-IP call.”

With respect to the positive and welcomed uses affiliated with “Caller ID Spoofing” such as research, investigative tactics, and public services, it is my recommendation as a representative of the information security community that the exemption to this Bill be either expanded to include the above mentioned uses, or that the term “illicit” be added to the general wording of the Bill. This way, the legitimate academic and commercial entities (and the law enforcement agencies they aid) will not unduly suffer the effects of this proposed Act.

The implementation of “The Truth in Caller ID Act of 2006” will without a doubt prove to be instrumental in the fight against the criminal activities in, and the abuse of, our nation's telephone communication systems. By recognizing this Bill as an amendment to the “Communications Act of 1934”, our government will continue to send the message of intolerance towards those who seek to take advantage of burgeoning technologies for illegal and/or unethical use.

Lance James
Chief Technology Officer
Secure Science Corporation